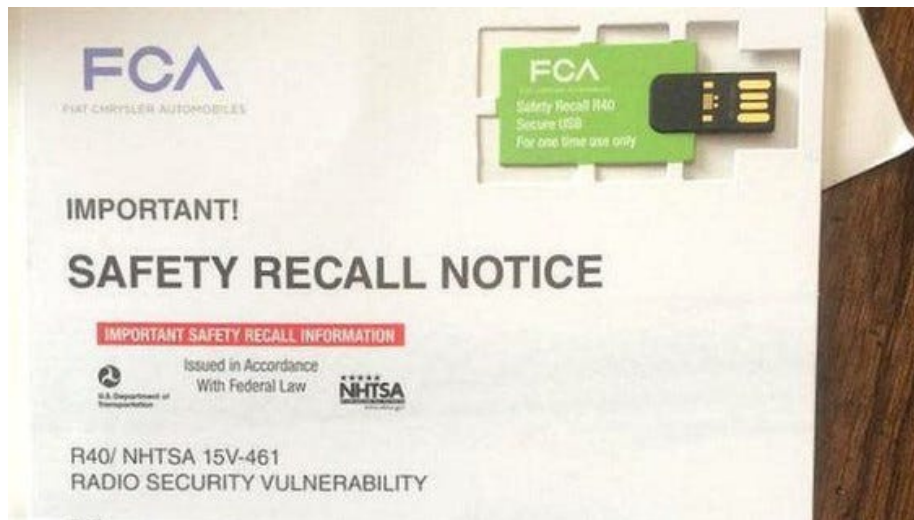
Cassandra Crossing/ La sicurezza secondo Marchionne

(355)—La campagna di aggiornamento per le vetture FCA vulnerabili avviene a mezzo chiavetta USB, spedita per posta. Aprendo il campo ad…

Cassandra Crossing/ La sicurezza secondo Marchionne

(355)—La campagna di aggiornamento per le vetture FCA vulnerabili avviene a mezzo chiavetta USB, spedita per posta. Aprendo il campo ad una nuova vastissima superficie d'attacco.

18 settembre 2015—Anche stavolta l'AD di FCA viene citato non per sua personale responsabilità, ma perché il caso Jeep, già recentemente oggetto dell'attenzione di Cassandra, è il più recente e l'unico "attenzionato" dai media italiani.

Ed anche stavolta non è un problema solo di FCA (vedi i casi di General Motors e Tesla), ma del complesso di un'industria, quella dell'automotive, in cui la sicurezza degli utenti è gestita sì abbastanza correttamente (anche se non necessariamente bene) per gli aspetti meccanici ed elettronici, ma è invece ancora profondamente incompresa, trascurata e spesso ignorata nei processi produttivi sotto quelli informatici e telematici.

"Cosa è successo stavolta?", sospireranno i 24 incerti lettori.

Beh, in fondo niente di particolare, visto che FCA ha fatto, per il richiamo delle auto coinvolte, esattamente quello che aveva annunciato: invece di eseguire il

costosissimo richiamo di un milione di vetture, ha iniziato ad inviare una chiavetta USB in una lettera contenente le istruzioni per applicare il fix, spendendo ovviamente meno ed agevolando i suoi clienti, che non dovranno prendere appuntamenti e recarsi in officina.

L'iniziativa sembra degna di lode: per semplicità ed economicità lo è certamente.Ma parlando invece di sicurezza, la possiamo definire un buon caso di studio, un "buon cattivo esempio". E spieghiamo perché.

In un caso analogo, General Motors ha reso la patch software disponibile sul proprio sito: scaricarla e copiarla su una chiavetta da almeno 4GB veniva lasciato all'utente.

FCA in questo caso ha invece inviato per posta normale, agli indirizzi registrati dei proprietari dei veicoli, una chiavetta del tipo punzonato già col software caricato. La busta, ahimè, è facilmente riconoscibile, e la chiavetta punzonata è stata fotografata ed ampiamente diffusa dai media.

Questo apre quello che si chiama una “superficie di attacco” integralmente nuova, perché di tipo non informatico ma “postale”: cosa impedisce di intercettare la lettera dalla cassetta di posta del vicino, cancellare la patch contenuta, sostituirvi un software malevolo e rimetterla a posto?

Cosa impedisce di sottrarne un centinaio dal camion di un corriere od un numero ancora maggiore dall’ufficio postale di spedizione e ripetere l’operazione?

Cosa impedisce di falsificare una intera campagna di richiamo? Assolutamente nulla: la busta di FCA non è anonima, come sono invece quelle di una nuova carta di credito, quindi è ben individuabile e se necessario imitabile. Anche la chiavetta lo è.Niente impedisce di utilizzare il sistema anche per futuri attacchi, non di massa ma mirati ad una particolare persona.

Per non aprire quindi un nuovo “vettore di attacco”, è necessario chiudere la nuova “superficie di attacco” postale con una contromisura informatica che la neutralizzi completamente.

Ogni auto potrebbe, per esempio, essere dotata di una chiave crittografica privata diversa, e la patch potrebbe essere crittografata per tutte le chiavi esistenti in modo da essere non falsificabile e non alterabile.

Se qualcuno dei 24 lettori avesse il dubbio se si può crittografare un file per un milione di chiavi, sì, si può: basta pensare a come funziona ad esempio, la cifratura di PGP, che usa contemporaneamente sia chiavi simmetriche che asimmetriche proprio per poter cifrare per più destinatari in maniera efficiente.

Cassandra può avere una sua opinione in merito, ma non conoscendo nulla dello specifico evento e della soluzione distribuita si limita a dire che se la patch è stata distribuita in questo modo (o con uno equivalente) la nuova superficie di attacco “postale” è stata chiusa, e nessun nuovo “vettore di attacco” è stato creato.In caso contrario, distribuendo la patch per posta, si è offerta una nuova opportunità di creare nuovi ed economici vettori di attacco, facilitando moltissimo la vita ai cracker che volessero sfruttare gli exploit di bug nel software delle autovetture di FCA.

Solo come esempi teorici, si potrebbe pensare di ottenere una copia “virtuale” delle chiavi dell’auto, o a modifiche da romanzo di spie che permettano di comandare un colpo di sterzo o l’acceleratore a tavoletta quando il GPS e la telecamera di bordo comunicano che una certa auto è su un alto viadotto o si avvicina ad un incrocio a “T”.

Confidiamo che in tempi stretti tutto il settore automotive inizi a gestire correttamente e competentemente questo tipo di problemi.Sennò meglio la bicicletta, ma di quelle vecchie, senza aggeggi informatici.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica “Quattro chiacchiere con Cassandra”
Lo Slog (Static Blog) di Cassandra
L’archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 2, 2023.

Canonical link

Exported from Medium on January 2, 2024.